[redacted]

National Defense Industrial Association

14th Annual Security Technology Symposium and Exhibition

Williamsburg, Virginia
June 15-18, 1998

Economic Espionage Act of 1996: The Implications for Technology Transfer

Giovanna M. Cinelli, Esquire
Reed Smith Shaw & McClay LLP
8251 Greensboro Drive
McLean, Virginia 22102

ECONOMIC ESPIONAGE

- What is it?
  - ✦ industrial espionage versus aggressive competition
  - ✦ domestic versus international
- Legal responses?
  - ✦ theft statutes
  - ✦ intellectual property laws
  - ✦ Economic Espionage Act of 1996

[redacted]

STATISTICS

- Estimated losses: over $2 billion (American Society for Industrial Security
- FBI/DOJ responses: over 600 active cases through 1998
  - ✦ over 57 nations have been trying to obtain advanced technologies from U.S. corporations
  - ✦ active efforts by France, Japan, and Israel
  - ✦ Example companies affected: IBM, 3M Corporation, Eastman Kodak, Recon Optical; Avery Dennison, Bristol Meyer Squibb, AT&T, Gillette

[redacted]

ECONOMIC ESPIONAGE ACT OF 1996
§ § 1831 - 1839

- Designed to extend criminal jurisdiction to foreign governments, agents, parties or representatives who participate in activities which violate § § 1831-1832

[redacted]

EEA ELEMENTS
§ 1831

- Knowing "theft"
- By "fraud, artifice or deception"
- Of "trade secrets"
- "Carried away" or transmitted in any form
- To benefit any "foreign government, foreign instrumentality or foreign agent"

[redacted]

EEA ELEMENTS
(cont'd)

- A person who knowingly "copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates or conveys"
- A "trade secret"
- Without authorization
- For the benefit of a foreign government, agent or instrumentality

[redacted]

EEA ELEMENTS
(cont'd)

- Knowingly "receives, buys, or possesses"
- A "trade secret"
- "Knowing" it to have been "stolen or appropriated, obtained or converted without authorization"
- For the benefit of a foreign government, agent or instrumentality

[redacted]

EEA ELEMENTS
§ 1832

- "Whoever," with intent to convert a trade secret
- Theft, or without authorization, "takes, carries away, or conceals"
- By fraud, artifice or deception
- obtains such "trade secret" information

[redacted]

KEY DEFINITIONS

- Trade secret (§ 1839(3)):
  - ✦ "all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing"

OTHER REQUIREMENTS

- Trade secret owners must take reasonable measures to keep trade secret confidential

- The information (trade secret) derives "independent economic value, actual or potential" from not being known or readily ascertainable through public means

[redacted]

EXTRATERRITORIALLY APPLIED

- Statute applies to conduct outside the U.S. committed by a U.S. citizen or permanent resident

OR

to conduct by an organization organized under the laws of the U.S.

OR

if any act in furtherance of the offense was committed in the U.S.

APPROACH TO UTILIZATION OF THE STATUTE

- Risk analysis
- Technology or information involved
- Individuals with access, or likely access, to trade secret information
- Publicity
- Confidential protection of information once in the court system

METHODS OF COLLECTION WHICH PLACE INDUSTRY ON NOTICE OF POTENTIAL INDUSTRIAL ESPIONAGE

- Unsolicited requests for information through:
  - telephone
  - e-mail
  - fax
  - visit
- Request for response to marketing surveys
- Increased "hits" to company's Internet bulletin board or home page
- Inappropriate conduct during site visits
  - questions not directly related to visit
  - unusual number of methods of recording visits -- cameras, tape recorders, paper, laptops, handheld record compilers, dictaphones
  - unusual number of requests to make telephone calls
  - unusual attire
  - unusual qualifications of people on tour

[redacted]

COLLECTION METHODS (cont'd)

- Unsolicited requests by foreign persons to market services to research facilities, academic institutions or companies. Invitations by foreign parties for U.S. technical experts to visit foreign sites to share technical expertise; *i.e.*, tied to "employment opportunities," intellectual property collaboration
- International exhibits, shows, seminars or conventions
- Joint Ventures and other Collaborative Efforts:
  - ✦ extensive opportunity to exchange information
  - ✦ wary of lopsided exchanges
  - ✦ varying degrees of respect and enforcement of nondisclosure agreements
  - ✦ over-submission of information during joint venture or other collaborative efforts negotiations

AREAS OF FOREIGN INTEREST IN TECHNOLOGY
(U.S. Government Studies)

- Aeronautics systems
- Armaments and energetic materials
- Chemical and biological systems
- Directed and kinetic energy systems
- Electronics
- Ground systems
- Guidance, navigation, and vehicle control
- Information systems
- Information warfare
- Manufacturing and fabrication
- Marine systems
- Materials
- Nuclear systems
- Power systems
- Sensors and lasers
- Signature control
- Space systems
- Weapons effects and countermeasures

FOCUSED AREAS OF HEIGHTENED INTEREST
(DOE Perspective)

- Ceramics
- Cermets
- Refractories
- Advanced automotive propulsion
- Composite materials
- Nuclear radiation sources
- Safeguard methods for nuclear materials
- Superconductivity
- Uranium enrichment

PLUS

- Environmental sciences - terrestrial (1994)
- Biomedical sciences - basic studies (1995)

[redacted]

COMPANY EFFORTS TO LIMIT "TRADE SECRET" THEFT

- Due diligence on employee background
- Training/sensitization
- Certifications or acknowledgments in NDAs
- Limiting access to those who really need to

ECONOMIC ESPIONAGE ACT OF 1996

This law was signed by President Clinton on October 11, 1996, culminating a nearly two-year effort on the part of the FBI and U.S. industry professionals to understand the scope of and effectively deal with the foreign economic espionage problem affecting the USA. This law also addresses the theft of trade secrets where no foreign involvement is found. The FBI initiated the Economic Counterintelligence Program in late 1994 with a mission to collect information and engage in activities to detect and counteract foreign power sponsored or coordinated threats and activities directed against U.S. economic interests. This focused effort resulted in a dramatic increase in FBI investigations and a realization that existing legal remedies were insufficient to address the scope and nature of the economic espionage problem. The Economic Espionage Act of 1996 resolves many gaps and inadequacies in existing federal laws by specifically proscribing the various acts defined under economic espionage and addressing the national security aspects of this crime. Additionally, it provides for criminal forfeiture of proceeds obtained as the result of economic espionage, preserves confidentiality in any prosecution, and provides for extraterritorial jurisdiction.

ECONOMIC ESPIONAGE PROVISIONS

§1831 Economic Espionage [Agent of Foreign Power]
[Penalties: Persons: $500,000, 15 years; Organizations: $10,000,000]
a. IN GENERAL: Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly --
1. Steals, or without authorization appropriates, takes carries way or communicates, or by fraud, artifice, or deception obtain trade secrets;
2. Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
3. Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained or converted without authorization;
4. Attempts to commit any offense described in any of paragraphs 1 through 3; or
5. Conspires with one or more other persons to commit any offense described in any of paragraphs I through 4, and one or more of such persons do nay act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.
b. ORGANIZATIONS: Any organization that commits any offense described in subsection (a) shall be fined not more that $10,000,000.

§1832 Theft of Trade Secrets [Commercial Espionage]
[Penalties: Persons: $500,000, 10 years; Organizations: $5,000,000]
a. Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secrets knowingly --
1. Steals, or without authorizations appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtain such information;
2. Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
3. Receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
4. Attempts to commit any offense described in paragraphs 1 through 3;
5. Conspires with one or more other persons to commit any offense described in paragraphs 1 through 3, and one or more such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.
b. Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

§1833 Exceptions [Law enforcement activity is exempt]
This chapter does not prohibit --
1. Any otherwise lawful activity conducted by a governmental entity of the United States, a State, or political subdivision of a State; or
2. The reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

§1834 Criminal Forfeiture [Additional penalty of forfeiture]
a. The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States;
1. Any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
2. Any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violations, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.
b. Property subject of forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 8530), except for subsections d and j of such section. which shall not apply for forfeitures under this section.

§1835 Orders to Preserve Confidentiality
In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil procedures, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

§1836 Civil proceedings to enjoin violations

a. The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

b. The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

§1837 Applicability to Conduct Outside the US

This chapter also applies to conduct occurring outside the United States if

1. Offender is a natural person who is a citizen or permanent resident alien, or organization organized under the laws of the US.

2. An act in furtherance of offense was committed in the US.

§1838 Construction with Other Laws

This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly know as the Freedom of Information Act).

§1839 Definitions:

As used in this chapter --

1. The term "foreign instrumentality" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

2. The term "foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

3. The term "trade secret" means all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if --

A. the owner thereof has taken reasonable measures to keep such information secret; and

B. the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

4. The term "owner," with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

b. CLERICAL AMENDMENT -- The table of chapters at the beginning part 1 of title 18, United States Code, is amended by inserting after the item relating to chapter 89 the following: 1831.

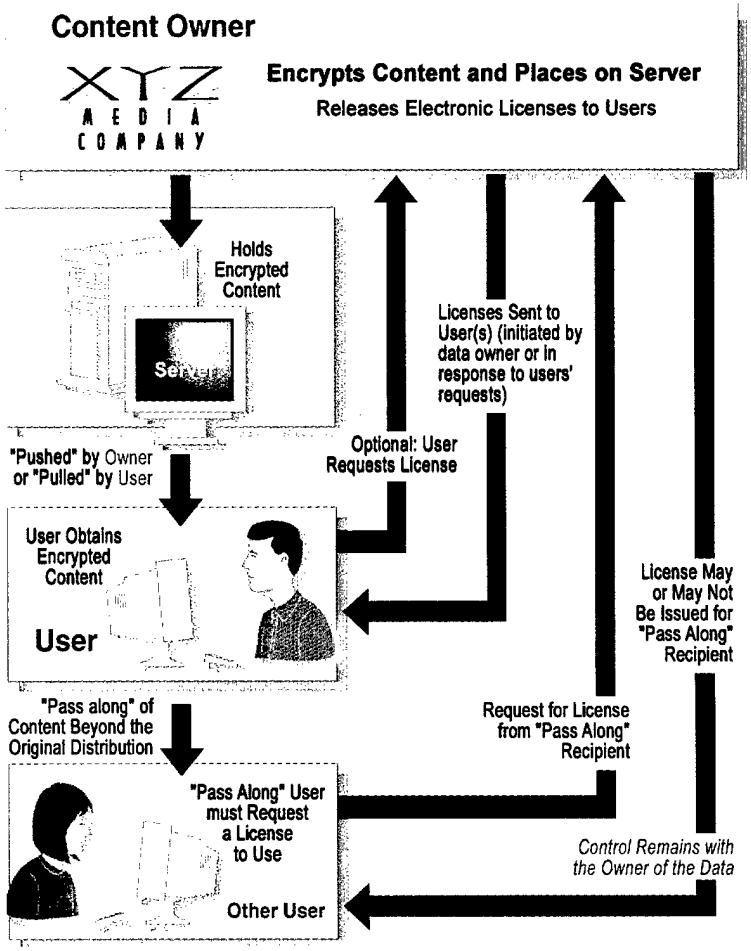
c. REPORTS -- Not later than 2 years and 4 years after the date of the enactment of this Act, the Attorney General shall report to Congress on the amounts received and distributed from fines for offenses under this chapter deposited in the Crime Victims' Fund established by section 1402 of the Victims of Crime Act of 1984 (42 U.S.C 10601).

Persistent Access Control or *How to Retain Control of Your Data After Delivery*

Today we can deliver information to users while safeguarding its confidentiality, ensuring its authenticity, and validating its origin. However, once information has been delivered, the originator must rely on the trusted behavior of the end user. Each user represents a vulnerability where copying or redistribution can occur. To protect information, we must forego many opportunities to use it. MRJ's technology breakthrough allows an originator to maintain control of information even after it has been delivered. In fact, the solution described here allows information to be posted and openly distributed (in encrypted form), allowing access only to authorized users and only as defined by the originator.

The three components of this invention[1] are:

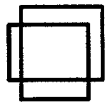
- originator-*encrypted* information (where the key is known only to the originator).
- *electronic licenses* that control who may access the information as well as the specific accesses that are permitted (e.g., read-only, printing, display resolution, copying, time and duration of access, etc.).
- *hardware access mechanism* that mediates all input/output (access) requests—allowing only those permitted by the electronic license. A PC augmented with the hardware access mechanism would be compatible with current software and files. A tamper-detecting capability denies physical access to the hardware mechanism or to cryptographic variables.



Some of the major benefits provided by this technology are described below. Pass through or secondary distribution remains under control of the originator. This means that a report *cannot* be copied, printed, or retransmitted beyond the individuals or offices on the original distribution list. Further, an originator can control access to products based on the originator's data. Any recipient of such a product may be required to obtain an electronic license from the owner of the original. Controlling the user's ability to copy, print, or retransmit sharply reduces the opportunity for leaks or redistribution.

Distribution logistics are dramatically improved. A file can contain items at multiple classifications and in different compartments. Images might be available at different resolutions or in different geographical areas. Users will be able to access only those parts which their license allows. Isolation is guaranteed because a user receives keys only to those compartments (or resolutions or areas) for which he or she has access approval. Software execution can also be controlled. In the electronic license, the software originator can specify the specific features available to each user or class of users.

Because the system operates with standard PC hardware and software and any media (e.g., CD-ROM, DVD), it will not stagnate, but will continue to benefit from and evolve with advances in the underlying technology of the PC.



MRJ Technology Solutions

Paul B. Schneck (703) 277-1618
schneck@mrj.com

[1] Based on technology developed at the MITRE Corporation by Paul B. Schneck with Marshall Abrams.